



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/747,687	12/22/2000	Xun Wilson Huang	21816-04953	4655

7590 12/01/2004

JEFFREY BRILL  
FENWICK & WEST LLP  
SILICON VALLEY CENTER  
801 CALIFORNIA STREET  
MOUNTAIN VIEW, CA 94041

EXAMINER

ZHEN, LI B

ART UNIT PAPER NUMBER

2126

DATE MAILED: 12/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/747,687

Applicant(s)

HUANG ET AL.

Examiner

Li B. Zhen

Art Unit

2126

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 24 August 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-58 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-58 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>8/26/04 and 10/19/04</u> | 6) <input type="checkbox"/> Other: _____  |

**DETAILED ACTION**

1. Claims 1 – 58 are pending in the application.

***Claim Rejections - 35 USC § 102***

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. **Claims 1, 3 – 8, 13 – 16, 18, 21, 23 – 28, 33 – 36, 38, 41, 43 – 48, 53 – 56 and 58 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent NO. 6,161,139 to Win [cited in previous office action].**

4. As to claim 1, Win teaches a method for virtualizing super-user privileges [administrative roles; col. 2, line 65 – col. 3, line 20] in a computer operating system including multiple virtual processes [plurality of users; col. 2, line 65 – col. 3, line 20], the method comprising:

designating a plurality of virtual super-users [when the Admin Role is assigned to a user, that user has the right to perform administrative functions; col. 15, line 60 – col. 16, line 55], each virtual super-user being associated with a separate virtual process [associates a user with one or more of the administrative roles, and that associates

Art Unit: 2126

each administration role with one or more administrative privileges; col. 2, lines 52 – 66];

intercepting a system call for which actual super-user privileges are required [when the user selects a resource, the browser sends an open URL request and cookie to a Protected Web Server...a Protected Web Server is a web server with resources protected by the Runtime Module...the Runtime Module decrypts information in the cookie and uses it to verify that the user is authorized to access the resource; col. 6, lines 33 – 46]; and

in response to the intercepted system call [when the user requests the execution of an administrative function; col. 2, lines 50 – 66] being made by a virtual super-user [user's administrative roles] and pertaining to the virtual process of the virtual super-user [the requests is honored only when one of the user's administrative roles includes an administrative privilege that authorizes the requested administrative function; col. 2, lines 50 – 66]:

granting actual super-user privileges to the virtual super-user [user's administrative roles includes an administrative privilege that authorizes the requested administrative function; col. 2, lines 50 – 66]; and

allowing execution of the system call [when the Admin Role is assigned to a user, that user has the right to perform administrative functions; col. 15, line 67 – col. 16, line 25].

5. As to claim 3, Win teaches assigning a virtual super-user identifier to each virtual super-user [administrative Role ID value uniquely identifies the Admin Role; col. 16, lines 9 – 25].

6. As to claim 4, Win teaches each virtual super-user identifier comprises a super-user identifier and an indication of a virtual process [to create an association of a role to the selected resource, a user selects one of the roles 1028a-1028n from the list 1026 and selects the Assign button 1036; col. 18, lines 13 – 25].

7. As to claim 5, Win teaches assigning a user identifier to a virtual super-user [a user selects one of the roles 1028a-1028n from the list 1026 and selects the Assign button 1036; col. 18, lines 13 – 25] and storing the user identifier and an indication of the virtual process of the virtual super-user in a virtual super-user list [Administration Application 114 displays the selected role (such as "Sales Manager") in the assigned roles list 1024; col. 18, lines 13 – 26].

8. As to claim 6, Win teaches assigning a super-user identifier [Administrative Role ID value uniquely identifies the Admin Role; col. 16, lines 10 – 23] to the virtual super-user [when the Admin Role is assigned to a user, that user has the right to perform administrative functions; col. 15, line 67 – col. 16, line 6].

Art Unit: 2126

9. As to claim 7, Win teaches the intercepted system call comprises a system call ["Open the Resource designated by this URL"; col. 7, lines 52 – 67] for accessing a file [list of protected resources may identify resources by a literal name, such as a file name of an executable program; col. 14, lines 54 – 67].

10. As to claim 8, Win teaches the intercepted system call pertains to the virtual process of the virtual super-user when the file to be accessed is associated with the same virtual process [Role Admin privilege may be delegated to owners of a particular resource; col. 16, lines 57 – 67].

11. As to claim 13, Win teaches the system call is made by a virtual super-user when a user making the call has a virtual super-user identifier [Admin Role is assigned to a user, that user has the right to perform administrative functions; col. 16, lines 1 – 25].

12. As to claim 14, Win teaches the system call is made by a virtual super-user [a user selects one of the roles 1028a-1028n from the list 1026 and selects the Assign button 1036; col. 18, lines 13 – 25] when a user making the call has a user identifier in a virtual super-user list [Administration Application 114 displays the selected role (such as "Sales Manager") in the assigned roles list 1024; col. 18, lines 13 – 26].

13. As to claims 15, Win teaches responsive to the intercepted system call not being made by a virtual super-user, disallowing execution of the system call [If the conditions

Art Unit: 2126

are not satisfied, then the user cannot be authenticated, and as shown in state 314, Runtime Module 206 returns a redirection to the Login URL; col. 8, lines 3 – 17].

14. As to claim 16, Win teaches responsive to the intercepted system call being made by a virtual super-user and not pertaining to the virtual process of the virtual super-user, disallowing execution of the system call [If the conditions are not satisfied, then the user cannot be authenticated, and as shown in state 314, Runtime Module 206 returns a redirection to the Login URL; col. 8, lines 3 – 17].

15. As to claim 18, Win teaches allowing comprises: executing [perform administrative functions] the system call [when the Admin Role is assigned to a user, that user has the right to perform administrative functions; col. 15, line 67 – col. 16, line 25].

16. As to claims 21, 23 – 28, 33 – 36 and 38, these are product claims that correspond to method claims 1, 3 – 8, 13 – 16 and 18; note the rejections to claims 1, 3 – 8, 13 – 16 and 18 above, which also meet these product claims.

17. As to claims 41, 43 – 48, 53 – 56 and 58, these are system claims that correspond to method claims 1, 3 – 8, 13 – 16 and 18; note the rejections to claims 1, 3 – 8, 13 – 16 and 18 above, which also meet these systems claims.

***Claim Rejections - 35 USC § 103***

18. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

19. **Claims 2, 22 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Win in view of U.S. Patent NO. 6,578,055 to Hutchison [cited in previous office action].**

20. As to claims 2, 22 and 42, Win teaches withdrawing super-user privileges [If multiple roles are displayed in the assigned roles list 1024, and the administrator wishes to remove all of them, the administrator may either press the Unassign button 1034 multiple times until all roles are un-assigned; col. 18, lines 33 – 45] but does not specifically teach withdrawing the actual super-user privileges from the virtual super-user after execution of the system call.

However, Hutchison teaches virtualizing super-user privileges in a computer operating system [a user level field of a data structure associated with the communication may be set to specify a root user level, such as 0; col. 3, lines 5 – 11], intercepting a system call for which actual super-user privileges are required [accesses to a file system are intercepted (block 200), Fig. 5; col. 8, lines 25 – 45], granting actual super-user privileges to the virtual super-user [the user level identified in the data structure accompanying the access is modified to the privileged user level, such as by



setting the user level field to 0 (block 206), Fig. 5; col. 8, lines 43 – 54], allowing execution of the system call [access with the modified data structure is then forwarded to the file system (block 208), Fig. 5; col. 8, lines 43 – 54], and withdrawing the actual super-user privileges from the virtual super-user after execution of the system call [when the file mirroring operation completes (block 104) the privileged user level may be released (block 106); col. 8, lines 23 – 45].

21. It would have been obvious to a person of ordinarily skilled in the art at the time of the invention to apply the teaching of withdrawing the actual super-user privileges from the virtual super-user after execution of the system call as taught by Hutchison to the invention of Win because this provides privileged user level only when needed and reduces the risk of having a process at the root user level [col. 8, lines 23 – 31 of Hutchison].

**22. Claims 9 – 12, 17, 19, 20, 29 – 32, 37, 39, 40, 49 – 52 and 57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Win in view of U.S. Patent NO. 6,658,571 to O'Brien [cited in previous office action].**

23. As to claim 9, Win teaches beginning and ending sessions [Authentication Client Module 414 enables users to begin and end authenticated sessions; col. 9, lines 17 – 25] but does not teach terminating a process.

However, O'Brien teaches a system call wrapper intercepting system calls from applications [mechanism for dynamically wrapping standard, commercially available

Art Unit: 2126

software application; col. 2, lines 10 – 39], invoking one or more security modules to process the system call [col. 2, lines 28 – 36], and a system call to terminate a process [close module 411 releases all the kernel buffers that were acquired and unregisters security module 105; col. 6, lines 17 – 36].

24. It would have been obvious to a person of ordinarily skilled in the art at the time of the invention to apply the teaching of a system call to terminate a process as taught by O'Brien to the invention of Win because this allows a process and its resources to be released when the process is no longer needed [release all the kernel buffers; col. 6, lines 30 – 32 of O'Brien].

25. As to claim 10, Win as modified teaches the intercepted system call pertains to the virtual process of the virtual super-user when the process to be terminated is associated with the same virtual process [a security module 105 unregisters itself via the API, security master 103 removes it from list 207; col. 5, lines 1 – 27 of O'Brien].

26. As to claim 11, Win as modified teaches identifying each process associated with the virtual process [close module 411 releases all the kernel buffers that were acquired and unregisters security module 105; col. 6, lines 17 – 36 of O'Brien], and terminating each identified process [a security module 105 unregisters itself via the API, security master 103 removes it from list 207; col. 5, lines 1 – 27 of O'Brien].

Art Unit: 2126

27. As to claim 12, Win as modified teaches a data structure [assigned roles list] stores associations between processes and virtual processes, and identifying each process by its association with the virtual process in the data structure [Administration Application 114 displays the selected role (such as "Sales Manager") in the assigned roles list 1024; col. 18, lines 13 – 26 of Win].

28. As to claim 17, Win as modified teaches responsive to the intercepted system call comprising a system call for inserting a module [malicious software] into an operating system kernel, disallowing execution of the system call [each security module 105 "wraps" one or more applications 107 in the sense that applications 107 cannot access computing resources 106 for which they are unauthorized in the event that an application 107 executes malicious software; col. 3, lines 39 – 56 of O'Brien].

29. As to claim 19, Win as modified teaches loading a system call wrapper [Security modules 105 are kernel-loadable modules that make and enforce application-specific or resource-specific policy decisions for applications 107; col. 3, lines 38 – 56 of O'Brien], saving a pointer to the system call [each entry includes the following fields: a pointer to the original system call handler within the operating system; col. 5, lines 27 – 46 of O'Brien] and replacing the pointer to the system call with a pointer to the system call wrapper, such that the system call wrapper is executed when the system call is invoked [for each system call being wrapped, security master 103 redirects each pointer from

Art Unit: 2126

the standard handler within the operating system to a corresponding system call wrapper within security master 103; col. 5, lines 27 – 46 of O'Brien].

30. As to claim 20, Win as modified teaches the pointer to the first system call comprises a system call vector [Conventional operating systems include a system call table (ST) that contains pointers to handlers for the various system calls; col. 5, lines 28 – 46 of O'Brien].

31. As to claims 29 – 32, 37, 39 and 40, they are rejected for the same reasons as claims 9 – 12, 17, 19 and 20 above.

32. As to claims 49 – 52 and 57, they are rejected for the same reasons as claims 9 – 12, and 17 above.

### ***Response to Arguments***

33. Applicant's arguments filed August 24, 2004 have been fully considered but they are not persuasive.

In response to the Non-Final Office action mailed on March 25, 2004, applicant argues:

(1) the claimed invention enables resource ownership in the context of multiple virtual private servers, specifically to a method for granting a user of a virtual process

Art Unit: 2126

(such as a virtual private server) super-user privileges without comprising system security [p. 14, lines 22 – 25];

(2) Win does not disclose associating anything with a process, whether it be a user, a super-user, an administrative role, an administrative privilege, or an administrative function [p. 15, lines 10 – 12]; and

(3) Win does not disclose associating anything with a virtual process [p. 15, line 12].

As to argument (1), it is noted that the features upon which applicant relies (i.e., virtual private servers) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims.

As to argument (2), examiner respectfully disagrees and notes that it is inherent that there is a process associated with a user in order for the operating system to process the user's input. For example, Win teaches that when a user selects a resource, the browser sends an open URL request and cookie to a Protected Web Server [col. 6, lines 33 – 46]. In this case, the browser is a client process associated with the user [col. 4, lines 46 – 57]. Therefore, Win teaches associating a user with a process.

In response to argument (3), examiner notes that the term "virtual process" is very broad. Although it appears that it is the applicant intension for a virtual process to mean a virtual private server, examiner notes that this is not brought out in the claims.

Art Unit: 2126

Therefore, broadly interpreted Win's browser client process would read on a virtual process.

***Conclusion***

34. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

35. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Li B. Zhen whose telephone number is (571) 272-3768. The examiner can normally be reached on Mon - Fri, 8:30am - 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Meng-Ai An can be reached on (571) 272-3756. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2126

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Li B. Zhen  
Examiner  
Art Unit 2126

lbz

  
MEI Q. T. AN  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100